Remarks

In the Final Office action mailed May 16, 2007, claims 1-7 were again rejected under 35 U.S.C. § 101 on grounds that the claimed invention is directed to non-statutory subject matter. In particular, with respect to Applicants' previous arguments, the Office action asserts that the claim as a whole can be reasonably interpreted as just solving a mathematical algorithm rather than reciting a practical application of the algorithm, and further states that the invention "would appear to be **concrete** and **tangible** in the context of the claim; however, the **useful** result appears to be lacking." Thus, it seems that the basis of the rejection is that these claims can be broadly interpreted to include non-statutory subject matter, so that the claims need to be amended to recite some specific and substantial use of the mathematical algorithm, in order to limit their scope to a practical application, thereby excluding any non-statutory matter from the claim.

Applicants amend independent claim 1 to recite a real-world use for the method of operating the multiplication circuit, namely in a cryptographic application. Further, claim 1 now recites a useful result of that method of operating the multiplication circuit, namely, fewer memory accesses. Thus, the invention clearly produces a useful result, in addition to a concrete and tangible result, in the context of the claim as now amended. As previously argued, the specification recites the use of the multiplication hardware in cryptographic applications (e.g., page 2, lines 3-15 and page 11, line 34 to page 12, line 3). It is in this field that the present claimed method is of particular real-world advantage over prior methods. In cryptography, there is need to multiply very large integers comprising a large number of words (e.g., 1024 words, by 1024 bits), values that are

much wider than the multiplication circuit. In cryptographic applications, the operands being operated upon by the multiplication circuit hardware represent message blocks, cryptographic keys and other such cryptographic data, and the required computations can be quite intensive. Efficient operation of the multiplication circuit has substantial practical results in terms of the time required for encrypting, decrypting, hashing, or the like. A circuit requiring fewer memory accesses is of significant advantage because it leads to efficient operation upon the multi-word operands in that cryptographic context. (Page 3, lines 1-4; page 4, lines 5-16; page 11, lines 8-11). This real-world advantage or useful result is now recited in the context of the claim.

In light of the amendments, the rejection under 35 U.S.C. § 101 is believed to be traversed.

Conclusion

Applicants thank the Examiner for the allowance of claim 8 and also for the indication of allowability of claims 1-7 over the prior art. Applicants request entry of the amendment (no new searching would be required), as it is believed to place the application in condition for allowance. Reconsideration of the section 101 rejection is hereby requested and a Notice of Allowance is earnestly solicited.

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) on the date shown below.

Signed: Sally Azevedo
Typed Name: Sally Azevedo

Date: June 19, 2007

Respectfully submitted,

D. M. Schneck

David M. Schneck
Reg. No. 43,094

Schneck & Schneck
P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733

ATM78:214.AAF